Shannon's theory of Perfect Secrecy

Outline

- Measure of Security of cryptosystems
- Perfect Secrecy
- Shift cipher
  - Security analysis
- One time pad
  - Security analysis

Definitions of security

- Computational Security
  - Adversary is computationally bounded
  - The best known algorithm required at least a large number of operations N
  - Can only be proved against specific attacks
- Provable Security
  - Proof by means of reduction to a well known problem that is thought to be hard
  - Examples ???
- Unconditional Security
  - Adversary has unlimited power

Definitions of security…

- Which one do you think is the best?
  - Then why don't we use it in practical scenarios ?

Unconditional Security

- Concerns the security of cryptosystems when the adversary has unbounded computational power
- Cipher-text only attack
  - Attack the cipher using cipher texts only
- When is the cipher unconditionally secure?

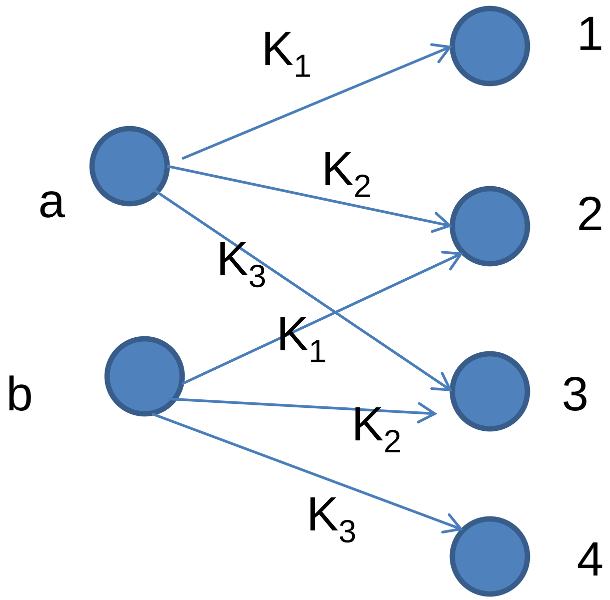
A priory and a posteriori probabilities

- Consider a cryptosystem (P,C,K,E,D)
- The plaintext has a probability distribution
- Pr(x) : a priori probability of a plain text
- The key also has a probability distribution
- Pr(K): a priori probability of a key
- The cipher text is generated by applying the encryption function .
  - Thus y= $E_k(x)$ is the cipher text
- The plaintext and the key are independent distributions

Attacker wants to compute a posteriori probability of a plaintext

- The probability distribution on P and K, induce a probability distribution on C, the cipher text
- For a key K, $C_K(x) = \{E_K(x): x \in P\}$
- Does the cipher text leak information about the plaintext?
  - Given a ciphertext y, we shall compute the a posteriori probability of the plain text, i.e. $P(x|y)$ and see whether it matches with tat of the a priori probability of the plain text

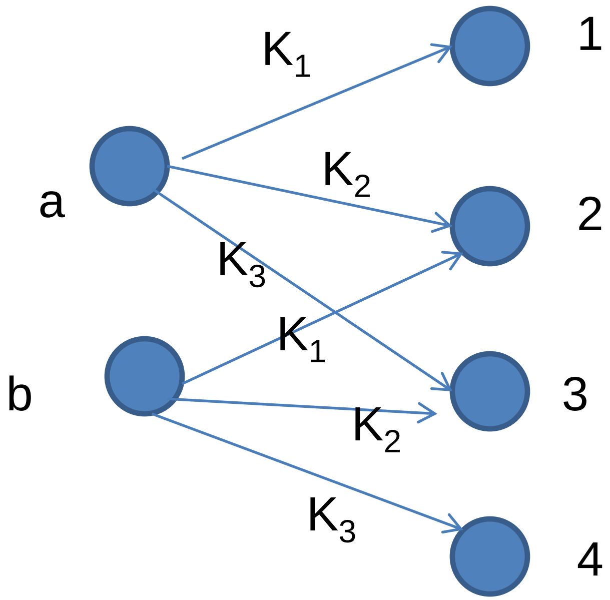
Example



	a	b
K_1	1	2
K_2	2	3
K_3	3	4

- $P=\{a,b\}$, $P_P(a) = ¼$, $P_P(b)=3/4$
- $K=\{K_1,K_2\}$, $P_K(K_1)=1/2$, $P_K(K_2)=P_K(K_3)=1/4$
- $C=\{1,2,3,4\}$
  - What is the a posteriori probability of Plaintext gince cipher texts from C?

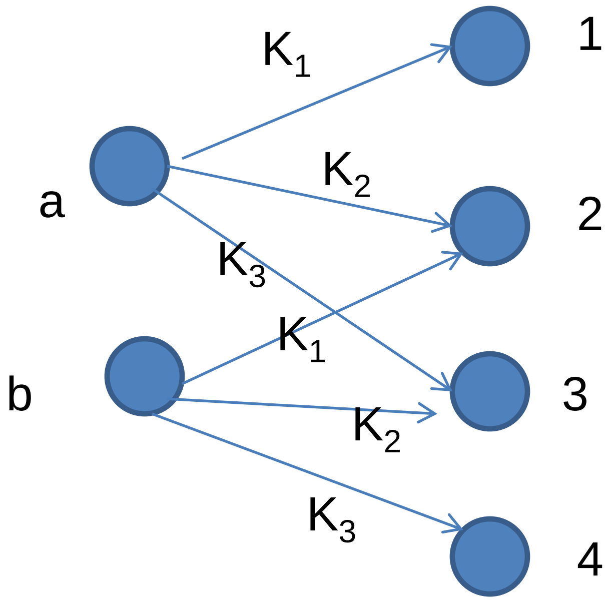
Example...



- $P=\{a,b\}$, $P_P(a) = ¼$, $P_P(b)=3/4$
- $K=\{K_1,K_2\}$, $P_K(K_1)=1/2$, $P_K(K_2)=P_K(K_3)=1/4$
- $C=\{1,2,3,4\}$

- $P_C(1)= P_P(a)\ P_K(K_1)=1/8$
- $P_C(3)= P_P(a)\ P_K(K_3) + P_P(b)\ P_K(K_2) =1/4$
- $P_C(2)=?$
- $P_C(4)= ?$

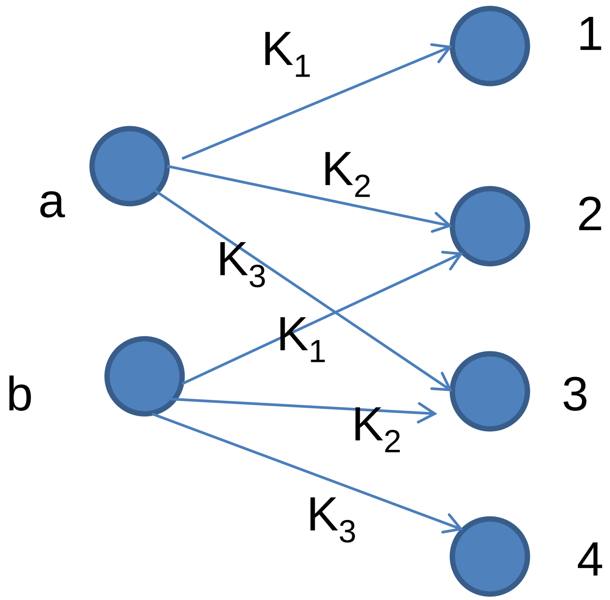
Example...



- $P=\{a,b\}$, $P_P(a) = ¼$, $P_P(b)=3/4$
- $K=\{K_1,K_2\}$, $P_K(K_1)=1/2$, $P_K(K_2)=P_K(K_3)=1/4$
- $C=\{1,2,3,4\}$

- $P_C(1)= P_P(a)\ P_K(K_1)=1/8$
- $P_C(3)= P_P(a)\ P_K(K_3) + P_P(b)\ P_K(K_2) =1/4$
- $P_C(2)=7/16$
- $P_C(4)= 3/16$

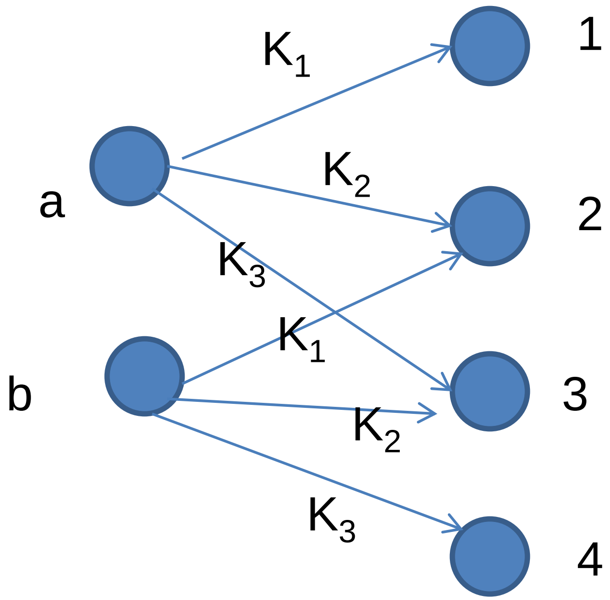
Example…



- $P=\{a,b\}$, $P_P(a) = ¼$, $P_P(b)=3/4$
- $K=\{K_1,K_2\}$, $P_K(K_1)=1/2$, $P_K(K_2)=P_K(K_3)=1/4$
- $C=\{1,2,3,4\}$

- $P_P(a|1)= 1$; $P_P(b|1)=0$
- $P_P(a|2)=$?
- The 2 can come when the plaintext was a and the key was K_2 or when the plaintext was b and the key was K_1
- Given 2, we need to computed the probability that it came from a

Example…



- P={a,b}, $P_P(a)$ = ¼, $P_P(b)$=3/4
- K={K_1,K_2}, $P_K(K_1)$=1/2, $P_K(K_2)$=$P_K(K_3)$=1/4
- C={1,2,3,4}

- Given 2, we need to computed the probability that it came from a
- The 2 can appear with a probability:
  - By having a as the plaintext and K_2 as the key : (1/4)(1/4)=1/16
  - By having b as the plaintext and K_1 as the key : (3/4)(1/2)=3/8=6/16
  - $P_P(a|2)$= (1/16)/(7/16)=1/7

Generalization of the example

$$p_P(x \mid y) = \frac{p_P(x) \sum_{K: x = d_K(y)} p_K(K)}{\sum_{\{K: y \in C(K)\}} p_K(K)\, p_P(d_K(y))}$$

Perfect Security

- A cryptosystem has perfect secrecy if

  $P_P(x|y) = P_P(x)$ for all $x \in P$ and $y \in C$

- That is .... ???

Shift cipher has perfect secrecy

- Suppose 26 keys in a shift cipher are used with equal probability 1/26
  - Then for any plaintext distribution shift cipher has perfect secrecy
- $P=C=K=Z_{26}$
- Encryption function $y = E_K(X) = (X+K) \bmod 26$

Perfect Secrecy

$$p_P(x \mid y) = \frac{p_P(x)\,p_C(y \mid x)}{p_C(y)}$$

$$p_C(y) = \sum_{K \in Z_{26}} p_K(K)\,p_P(d_K(y))$$

$$= \sum_{K \in Z_{26}} \frac{1}{26}\,p_P(y - K) = \frac{1}{26}$$

$$p_C(y \mid x) = P_K(y - x \bmod 26)$$

$$= \frac{1}{26}$$

- Perfectly secure if every ke is used with probability $1/|K|$
- And for every x and every y, there is a unique key such that $y=E_K(x)$
- Perfect secrecy : $P_C(y|x) = P_C(y)$